

ON THE CRITERIA OF THE F_5 ALGORITHM

CHRISTIAN EDER

ABSTRACT. Faugère's F_5 algorithm is one of the fastest known algorithms for the computation of Gröbner bases. So far only the F_5 Criterion is proved, whereas the second powerful criterion, the Rewritten Criterion, is not understood very well until now. We give a proof of both, the F_5 Criterion and the Rewritten Criterion showing their connection to syzygies, i.e. the relations between the S-Polynomials to be investigated by the algorithm. Using the example of a Gröbner basis computation stated in [Fau02] we show how Faugère's criteria work, and discuss the possibility of improving the F_5 Criterion.

1. INTRODUCTION

The F_5 algorithm stated in 2002 in [Fau02] is one of the fastest Gröbner basis algorithms up to date, but there are still not many implementations due to problems understanding the algorithm and its criteria to detect useless critical pairs of polynomials.

There are two main criteria: The F_5 Criterion and the Rewritten Criterion. Whereas proofs of the F_5 Criterion are given in [Fau02] and later on in a slightly different way also in [Ste05] there is still no proof for the Rewritten Criterion¹. Stegers tries to give an idea of how the criterion works, but he is not able to give a full proof.

In this paper we prove the correctness of both criteria and show that both are based on a similar relation between syzygies and interdependent S-Polynomials. Tightening the insight of the two criteria by giving examples and constructing the relations between the S-Polynomials using the ideas of the proof, this leads to an idea of an improvement of the F_5 Criterion also. We show that this improvement is not possible and there cannot be a generalization of the F_5 Criterion. Afterwards we explain the problem of connecting the discussed criteria with the 1st and 2nd Buchberger Criterion. This problem is strongly related to the dependence of Faugère's criteria on the signatures, whereas the Buchberger criteria do only care about the polynomial part of the critical pairs investigated.

The plan of this paper is the following: In Section 2 we give basic notations and definitions used in the F_5 algorithm. Section 3 includes the main theorem of this paper, Theorem 3.3 in whose proof the correctness of both, the F_5 Criterion and the Rewritten Criterion is shown. In the following we give for each criterion 3 detailed examples of how to use the constructive proof of Theorem 3.3 to see the correctness of deleting the detected pairs in the example given in [Fau02] Section 8. Afterwards we discuss the question of improving the F_5 Criterion on the basis of the constructive proof of the main theorem in Section 5 and show its failure. In the Appendix a short note on the current F_5 implementation in the computer algebra system SINGULAR is given.

Note that in this paper we do not state or prove the correctness or termination of any of the mentioned algorithms, we just prove the correctness of their criteria used, not the correctness and termination of the algorithms/implementations.

¹Recently Gash has given another proof of the Rewritten Criterion in [Gas08]

The proofs of the criteria are a joint work with John Perry. This paper represents my version of the results of our work. Another paper, which will include the discussion of the criteria as well as our discussion of the termination and correctness of F_5 , is in preparation by John Perry.

Acknowledgement.

The proofs of the criteria and the implementation of F_5 in a Singular library are joint work with John Perry.

2. BASIC CONCEPTS

First of all we need to state and understand the main definitions of Faugère's approach to work with polynomials during Gröbner bases computations. For this we need to find a relation between polynomials and module elements corresponding to them. This relation adds a new information to the polynomial which is later on used to decide if it is useful or not for the computation of a Gröbner basis.

2.1. Connection Between Polynomials And Module Elements. We state the main ideas of [Fau02] whereas we rewrite them in a slightly different way for the sake of simplicity.

Convention 2.1. In the following K is always a field, $\underline{x} = (x_1, \dots, x_n)$, \mathcal{T} denotes the set of terms of the ring $\mathbb{K}[\underline{x}]$. Let $F = (f_1, \dots, f_m)$ be a sequence of polynomials $F_i \in \mathbb{K}[\underline{x}]$ for $i \in \{1, \dots, m\}$ such that $I = \langle f_1, \dots, f_m \rangle$. Let $<$ denote a term order on $\mathbb{K}[\underline{x}]$.

Let $p_1, p_2 \in \mathbb{K}[\underline{x}]$, $u_k = \frac{\text{LCM}(\text{HT}(p_1), \text{HT}(p_2))}{\text{HT}(p_k)}$ for $k \in \{1, 2\}$ then we denote the S-Polynomial of p_1 and p_2 $\text{Spol}(p_1, p_2) = \text{HC}(p_2)u_1p_1 - \text{HC}(p_1)u_2p_2$.

Definition 2.2.

- (a) Let $\mathbb{K}[\underline{x}]^m$ be an m -dimensional module with generators $\mathbf{e}_1, \dots, \mathbf{e}_m$. Elements of the form $t\mathbf{e}_i$ such that $t \in \mathcal{T} \subset \mathbb{K}[\underline{x}]$ are called *module terms*. We define the *evaluation map*

$$\begin{aligned} v_F : \mathbb{K}[\underline{x}]^m &\rightarrow \mathbb{K}[\underline{x}] \\ \mathbf{e}_i &\mapsto f_i \quad \text{for all } i \in \{1, \dots, m\}. \end{aligned}$$

A *syzygy* of $\mathbb{K}[\underline{x}]^m$ is an element $\mathbf{s} \in \mathbb{K}[\underline{x}]^m$ such that $v_F(\mathbf{s}) = 0$.

- (b) We define the module term ordering \prec_F on $\mathbb{K}[\underline{x}]^m$:

$$t_i\mathbf{e}_i \prec_F t_j\mathbf{e}_j :\Leftrightarrow \begin{aligned} &(a) \quad i > j, \text{ or} \\ &(b) \quad i = j \text{ and } t_i < t_j \end{aligned}$$

- (c) For an element $\mathbf{g} = \sum_{i=1}^m \lambda_i \mathbf{e}_i \in \mathbb{K}[\underline{x}]^m$ we define the *index of \mathbf{g}* $\text{index}(\mathbf{g})$ to be the lowest number i_0 such that $\lambda_{i_0} \neq 0$. Let $\text{index}(\mathbf{g}) = k$, then the module head term of \mathbf{g} w.r.t. F is defined to be $\text{MHT}_F(\mathbf{g}) = \text{HT}(\lambda_k)\mathbf{e}_k$.
- (d) Let $p \in \mathbb{K}[\underline{x}]$ be a polynomial, we call p *admissible w.r.t. F* if there exists an element $\mathbf{g} \in \mathbb{K}[\underline{x}]^m$ such that $v_F(\mathbf{g}) = p$.
- (e) A *admissible w.r.t. F , labeled polynomial r* is an element of $\mathbb{K}[\underline{x}]^m \times \mathbb{K}[\underline{x}]$ defined by

$$r = (\mathcal{S}(r), \text{poly}(r))$$

where the components of r are defined as follows:

- (i) $\text{poly}(r) \in \mathbb{K}[\underline{x}]$ denotes the *polynomial part* of r . $\mathcal{S}(r)$ denotes the *signature* of r and is defined to be

$$\mathcal{S}(r) = \text{MHT}_F(\mathbf{g}) \text{ such that } v_F(\mathbf{g}) = \text{poly}(r).$$

- (ii) The *index* of r , $\text{index}(r)$ is defined to be $\text{index}(\mathbf{g})$ where

$$\text{MHT}(\mathbf{g}) = \mathcal{S}(r) \text{ and } v_F(\mathbf{g}) = \text{poly}(r).$$

- (f) Let r be an admissible w.r.t. F , labeled polynomial such that $\mathcal{S}(r) = t_i \mathbf{e}_i$. Then we define the *term of the signature* to be

$$\Gamma(\mathcal{S}(r)) = t_i.$$

- (g) Let $r_1 = (\mathcal{S}(r_1), \text{poly}(r_1))$ and $r_2 = (\mathcal{S}(r_2), \text{poly}(r_2))$ be two admissible labeled polynomials such that $u_2 \mathcal{S}(r_2) \prec_F u_1 \mathcal{S}(r_1)$. Then

$$\text{Spol}(r_1, r_2) = \left(u_1 \mathcal{S}(r_1), \text{Spol}(\text{poly}(r_1), \text{poly}(r_2)) \right)$$

Remark 2.3.

- (a) The notations MHT_F and \prec_F are due to distinguish Faugère's definition of a module term ordering in [Fau02] with the same approach in a different way of Möller, Traverso, and Mora in [MTM92], on which Faugère's ideas finding useless critical pairs is based on.
Note that the index F of MHT_F does not belong to the sequence F of polynomials in $\mathbb{K}[\underline{x}]^m$ also.
- (b) Note that the definition of the signature in 2.2(e) is different from Faugère's one in [Fau02]. Our understanding of a signature of a labeled polynomial r is equal to Faugère's definition of an admissible labeled polynomial r . This is due to the fact that the origin definition of the signature is not useful in the concept of computing Gröbner bases. Beside from Proposition 1 and Corollary 1 Faugère does not use his definition of the signature. When computing the Gröbner basis with the F_5 algorithm signatures are computed in the sense of Definition 2.2(e), hence we do not refer to Faugère's initially definition when speaking of the signature of an admissible w.r.t. F labeled polynomial, but to the definition given in this paper.
- (c) Note moreover that the signature $\mathcal{S}(r)$ of an admissible w.r.t. F , labeled polynomial r by Definition 2.2(e) is not uniquely defined.

Example 2.4. Assume the sequence $F = (f_1, \dots, f_m)$.

- (a) Let $p = f_1$. Then $r = (\mathbf{e}_1, f_1)$ is an admissible labeled polynomial as $v_F(\mathbf{e}_1) = f_1$.
- (b) Again let $p = f_1$. Then $r' = (f_2 \mathbf{e}_1, f_1)$ is also an admissible labeled polynomial. For this consider the module element $\mathbf{g} = (f_2 + 1) \mathbf{e}_1 - f_1 \mathbf{e}_2$. It holds that $v_F(\mathbf{g}) = f_2 f_1 + f_1 - f_1 f_2 = f_1$ and $\text{MHT}(\mathbf{g}) = f_2 \mathbf{e}_1$.

Remark 2.5. The F_5 Algorithm always takes the minimal possible index at the given iteration step during its computations. In the above situation the F_5 Criterion (see Definition 3.1) would detect and delete r' . This is an important point as in the case of F being a regular sequence all of these multiple descriptions of the signature can be detected and only the in some sense minimal one remains in the computations. Thus the signature computed by F_5 is unique in the case of an regular input.

Convention 2.6.

- (a) Due to the fact that in the following all labeled polynomials will be admissible w.r.t. F , we drop the reference to which set the admissibility is referred to for a shorter notation.
- (b) Let r be an admissible labeled polynomial. For a better legibility let in the following always denote $p = \text{poly}(r)$. So when referring to the signature and admissibility of an element we use the letter r , i.e. the labeled polynomial in $\mathbb{K}[\underline{x}]^m \times \mathbb{K}[\underline{x}]$, when considering the computations in terms of the polynomials itself we use the letter p , i.e. the polynomial in $\mathbb{K}[\underline{x}]$.

2.2. The Relation To Computations Of Gröbner Bases. To understand the two main criteria of the F_5 algorithm we embed $\mathbb{K}[\underline{x}]^m$ into the module $\mathbb{K}[\underline{x}]^{n_G}$ in a canonical way, i.e. $n_G \geq m$ and $\mathbb{K}[\underline{x}]^{n_G} = \mathbb{K}[\underline{x}]^m \times \mathbb{K}[\underline{x}]^{n_G-m}$.

Convention 2.7. In the following $G = \{r_1, \dots, r_{n_G}\}$ always denotes a set of admissible labeled polynomials such that $\text{poly}(G) := \{p_i \mid r_i \in G\} \supset \{f_1, \dots, f_m\}$. We assume that $r_i = (\mathbf{e}_i, f_i)$ for all $i \in \{1, \dots, m\}$ for the rest of this paper.

Definition 2.8.

- (a) We define an evaluation map

$$\begin{aligned} v_G : \mathbb{K}[\underline{x}]^{n_G} &\rightarrow \mathbb{K}[\underline{x}] \\ \mathbf{e}_i &\mapsto p_i \quad \text{for all } i \in \{1, \dots, n_G\}. \end{aligned}$$

A *syzygy* of $\mathbb{K}[\underline{x}]^{n_G}$ is an element $\mathbf{s} \in \mathbb{K}[\underline{x}]^{n_G}$ such that $v_G(\mathbf{s}) = 0$.

- (b) For each \mathbf{e}_i where $i \in \{1, \dots, n_G\}$ we define the module head term to be

$$\text{MHT}_F(\mathbf{e}_i) = \mathcal{S}(r_i)$$

as defined in 2.2(e) and 2.2(g).

Remark 2.9. Note that by Convention 2.7 $v_F(\mathbf{e}_i) = v_G(\mathbf{e}_i)$ for all $i \in \{1, \dots, m\}$.

Using admissible labeled polynomials to describe Gröbner bases for given ideals we need to define an admissible labeled equivalent to the t -representation known for polynomials in $\mathbb{K}[\underline{x}]$:

Definition 2.10. Let $r = (\mathcal{S}(r), p)$ be an admissible labeled polynomial, $\mathcal{M} = \{r_1, \dots, r_{n_{\mathcal{M}}}\}$ be a set of admissible labeled polynomials, and $t = \text{HT}(p)$. A representation

$$p = \sum_{j=1}^{n_{\mathcal{M}}} \lambda_j p_j, \quad \lambda_j \in \mathbb{K}[\underline{x}]$$

is an *admissible labeled t -representation* of (the admissible labeled polynomial) r if $\text{HT}(\lambda_j p_j) < t$ and $\text{HT}(\lambda_j) \mathcal{S}(r_j) \preceq_F \mathcal{S}(r)$ for all j .

There is an easy connection between usual and admissible labeled t -representations:

Lemma 2.11. *Let r be an admissible labeled polynomial. If r has an admissible labeled t -representation for $t = \text{HT}(p)$ then p has a t -representation.*

Proof. Clear by Definition 2.10. □

Convention 2.12. When speaking of an admissible labeled t -representation of an S-Polynomial $\text{Spol}(r_i, r_j)$ in the following without explicitly denoting t we always assume that $t = \text{LCM}(\text{HT}(p_i), \text{HT}(p_j))$.

It follows that we can give a new characterization of a Gröbner basis using admissible labeled polynomials.

Theorem 2.13. *If for all elements $r_i, r_j \in G$ $\text{Spol}(r_i, r_j)$ has an admissible labeled t -representation or $\text{Spol}(p_i, p_j)$ reduces to zero then $\text{poly}(G)$ is a Gröbner basis of $I = \langle f_1, \dots, f_m \rangle$.*

Proof. Clear by the characterization of a Gröbner basis and Lemma 2.11. \square

3. FAUGERE'S CRITERIA

Whereas a Gröbner basis G can be characterized by Theorem 2.13 it does not improve its computation, on the contrary we require even more, the polynomials need to be labeled and admissible w.r.t. a given set and their representations need to fulfill another criterion on their signatures. As the F_5 algorithm constructs new elements exactly such that they have admissible labeled t -representations, Faugère uses two criteria to check if the S-Polynomial of a critical pair needs to be computed and reduced, or if the critical pair is useless for the computation of G .

To decide if one of the criteria holds, the signatures of the labeled polynomials are used. By this means Faugère uses these new requirements on an admissible labeled t -representation stated in the previous section to get information on the relations between S-Polynomials which help to decide the necessity of them.

We state these criteria and prove their correctness, but we do not explain the F_5 algorithm in detail, we refer to [Fau02] or [Ste05] for a deeper insight in F_5 .

Definition 3.1 (F_5 Criterion). Let $(r_i, r_j) \in G \times G$ be a critical pair. $\text{Spol}(r_i, r_j)$ is *not normalized* iff for $u_k r_k$, $k = i$ or $k = j$, there exists $r_{\text{prev}} \in G$ such that

$$\begin{aligned} \text{index}(r_{\text{prev}}) &> \text{index}(r_k) \text{ and} \\ \text{HT}(p_{\text{prev}}) &| u_k \Gamma(\mathcal{S}(r_k)) \end{aligned}$$

If there exists no such $r_{\text{prev}} \in G$ then $\text{Spol}(r_i, r_j)$ is *normalized*.

Definition 3.2 (Rewritten Criterion). Let $(r_i, r_j) \in G \times G$ be a critical pair. $\text{Spol}(r_i, r_j)$ is *rewritable* iff for $u_k r_k$, $k = i$ or $k = j$, there exist $r_v, r_w \in G$ such that

$$\begin{aligned} \text{index}(r_k) &= \text{index}(\text{Spol}(r_v, r_w)) \text{ and} \\ \Gamma(\mathcal{S}((\text{Spol}(r_v, r_w)))) &| u_k \Gamma(\mathcal{S}(r_k)) \end{aligned}$$

If there exist no such $r_v, r_w \in G$ then $\text{Spol}(r_i, r_j)$ is called *not rewritable*.

Theorem 3.3. *Let $\mathcal{L} \subset G \times G$ be such that for each pair $(r_i, r_j) \in \mathcal{L}$ $\text{Spol}(r_i, r_j)$ is*

- (a) *normalized, and*
- (b) *not rewritable.*

Furthermore, if for each such pair $(r_i, r_j) \in \mathcal{L}$ $\text{Spol}(r_i, r_j)$ has an admissible labeled t -representation or $\text{Spol}(p_i, p_j)$ reduces to zero then $\text{poly}(G)$ is a Gröbner basis of $I = \langle f_1, \dots, f_m \rangle$.

Proof. Let $(r_i, r_j) \notin \mathcal{L}$. Then $\text{Spol}(r_i, r_j)$ is either not normalized or rewritable. We have to show that all such S-Polynomials either have an admissible labeled t -representation for $t = \text{LCM}(\text{HT}(p_i), \text{HT}(p_j))$ or reduce to zero.

We can assume that $u_j \mathcal{S}(r_j) \prec_F u_i \mathcal{S}(r_i)$ and w.l.o.g. we can assume that in each case $u_i r_i$ is the admissible labeled polynomial detected by one or both of the two criteria (see Remark 3.4). For this let $r_i = (t_i \mathbf{e}_k, p_i)$.

- (a) Assume that $u_i r_i$ is not normalized. In this case there exists an element r_{prev} in G with $\text{index}(r_{\text{prev}}) > k$ and $\Gamma(u_i \mathcal{S}(r_i)) = u_i t_i = \lambda \text{HT}(p_{\text{prev}})$ for some $\lambda \in \mathcal{T}$. This can be translated to a relation between two syzygies in $\mathbb{K}[\underline{x}]^{n_G}$: We receive a principal syzygy given by p_{prev} and f_k , namely

$$\mathbf{s}_{\text{prev},k} = p_{\text{prev}} \mathbf{e}_k - f_k \mathbf{e}_{\text{prev}} \in \mathbb{K}[\underline{x}]^{n_G}.$$

For r_i there are two possibilities:

- (i) If $i \in \{1, \dots, m\}$ then we can construct a trivial syzygy $\mathbf{s}_i = \mathbf{e}_i - \mathbf{e}_i$. Note that in this case $k = i$.
- (ii) If $i \notin \{1, \dots, m\}$ then r_i is the result of a reduction of an S-Polynomial, such that there exists a syzygy

$$\mathbf{s}_i = \sum_{\ell=k}^{n_i} a_{\ell}^i \mathbf{e}_{\ell} - \mathbf{e}_i$$

where n_i denotes the number of elements in the subsequent Gröbner basis G before r_i is added. It holds that $\text{MHT}_F(\mathbf{s}_i) = \mathcal{S}(r_i)$.

Either way $\text{MHT}_F(u_i \mathbf{s}_i) = \text{MHT}_F(\lambda \mathbf{s}_{\text{prev},k})$ by construction and we can compute their difference:

$$\begin{aligned} \lambda \mathbf{s}_{\text{prev},k} - u_i \mathbf{s}_i &= (\lambda \text{LOT}(p_{\text{prev}}) - u_i \text{LOT}(a_k^i)) \mathbf{e}_k + \sum_{\ell=k+1}^{n_i} a_{\ell}^i \mathbf{e}_{\ell} + \\ &\quad + \lambda f_k \mathbf{e}_{\text{prev}} - u_i \mathbf{e}_i. \end{aligned} \tag{1}$$

By construction

$$\begin{aligned} \text{HT}(\lambda \text{LOT}(p_{\text{prev}}) - u_i \text{LOT}(a_k^i)) \mathcal{S}(r_k) &\prec_F u_i \mathcal{S}(r_i) \\ \text{HT}(a_{\ell}^i) \mathcal{S}(r_{\ell}) &\prec_F u_i \mathcal{S}(r_i) \text{ for all } \ell \in \{k+1, \dots, n_i\} \\ \lambda \text{HT}(f_k) \mathcal{S}(r_{\text{prev}}) &\prec_F u_i \mathcal{S}(r_i). \end{aligned}$$

Note that in case (a)(i) $u_i \text{LOT}(a_k^i)$ is zero. As \mathbf{s}_i and $\mathbf{s}_{\text{prev},k}$ are syzygies it holds that $v_G(u_i \mathbf{s}_i - \lambda \mathbf{s}_{\text{prev},k}) = 0$.

- (b) Assume that $u_i r_i$ is rewritable. In this case there exists an $\text{Spol}(r_v, r_w)$ such that $\text{index}(\text{Spol}(r_v, r_w)) = k$ and $\lambda \in \mathcal{T}$ such that $\lambda \Gamma(\mathcal{S}(\text{Spol}(r_v, r_w))) = \Gamma(u_i \mathcal{S}(r_i))$. Again we can translate these data to a relationship between two syzygies. For r_i we have the same possibilities as mentioned in the case of $u_i r_i$ not normalized above, in short:

- (i) If $i \in \{1, \dots, m\} \Rightarrow \mathbf{s}_i = \mathbf{e}_i - \mathbf{e}_i$.
- (ii) If $i \notin \{1, \dots, m\} \Rightarrow \mathbf{s}_i = \sum_{\ell=k}^{n_i} a_{\ell}^i \mathbf{e}_{\ell} - \mathbf{e}_i$.

This time we also need to have a closer look at the syzygy given by $\text{Spol}(r_v, r_w)$. Based on the implementation of the Rewritten Criterion in the F_5 algorithm $\text{Spol}(r_v, r_w)$ is not rewritable, as otherwise $\text{Spol}(r_i, r_j)$ would be detected by the S-Polynomial which rewrites $\text{Spol}(r_v, r_w)$. $\text{Spol}(r_v, r_w)$ has been already or eventually will be reduced to a new element $r_{\text{rew}} \in G$, so it has a t -representation for $t < \text{LCM}(\text{HT}(p_v), \text{HT}(p_w))$, or it has been reduced to zero w.r.t. G . In either way we receive a syzygy

$$\mathbf{s}_{v,w} = \sum_{\ell=k}^{n_{\text{rew}}} a_{\ell}^{\text{rew}} \mathbf{e}_{\ell} - \alpha \mathbf{e}_{\text{rew}}$$

where n_{rew} denotes the number of elements in the subsequent Gröbner basis G before r_{rew} is possibly added. $\alpha = 0$ if $\text{Spol}(r_v, r_w)$ reduces to zero, and $\alpha = 1$ otherwise. It holds that $\text{MHT}_F(\mathbf{s}_{v,w}) = \mathcal{S}(\text{Spol}(r_v, r_w))$. Analogously to the case of $u_i r_i$ being not normalized we compute the difference of the two syzygies $u_i \mathbf{s}_i$ and $\lambda \mathbf{s}_{v,w}$ which fulfill the relation $\text{MHT}_F(u_i \mathbf{s}_i) = \text{MHT}_F(\lambda \mathbf{s}_{v,w})$:

$$\begin{aligned} \lambda \mathbf{s}_{v,w} - u_i \mathbf{s}_i &= (\lambda \text{LOT}(a_k^{\text{rew}}) - u_i \text{LOT}(a_k^i)) \mathbf{e}_k + \sum_{\ell=k+1}^{n_{\min}} (\lambda a_\ell^{\text{rew}} - u_i a_\ell^i) \mathbf{e}_\ell \\ &\quad + \sum_{\ell'=n_{\min}+1}^{n_{\max}} \lambda a_{\ell'}^{\text{rew}} \mathbf{e}_{\ell'} - \lambda \alpha \mathbf{e}_{\text{rew}} + u_i \mathbf{e}_i \\ &= (\lambda \text{LOT}(a_k^{\text{rew}}) - u_i \text{LOT}(a_k^i)) \mathbf{e}_k + \sum_{\ell=k+1}^{n_{\max}} (\lambda a_\ell^{\text{rew}} - u_i a_\ell^i) \mathbf{e}_\ell \\ &\quad - \lambda \alpha \mathbf{e}_{\text{rew}} + u_i \mathbf{e}_i \end{aligned} \tag{2}$$

where we define $n_{\min} = \min\{n_i, n_{\text{rew}}\}$, $n_{\max} = \max\{n_i, n_{\text{rew}}\}$. Note that in Equation (2)

$$\begin{aligned} a_\ell^i &= 0 \text{ for } \ell \in \{n_i + 1, \dots, n_{\max}\} \text{ or} \\ a_\ell^{\text{rew}} &= 0 \text{ for } \ell \in \{n_{\text{rew}} + 1, \dots, n_{\max}\}, \end{aligned}$$

depending on the relation of n_i and n_{rew} . It holds that $v_G(\lambda \mathbf{s}_{v,w} - u_i \mathbf{s}_i) = 0$, moreover

$$\begin{aligned} \text{HT}(\lambda \text{LOT}(a_k^{\text{rew}}) - u_i \text{LOT}(a_k^i)) \mathcal{S}(r_k) &\prec_F u_i \mathcal{S}(r_i) \\ \text{HT}(\lambda a_\ell^{\text{rew}} - u_i a_\ell^i) \mathcal{S}(r_\ell) &\prec_F u_i \mathcal{S}(r_i) \text{ for all } \ell \in \{k+1, \dots, n_{\max}\}. \end{aligned}$$

Note that $\lambda \mathcal{S}(r_{\text{rew}}) =_F u_i \mathcal{S}(r_i)$ by construction.

In both of the stated cases a new syzygy is built, we can summarize (1) and (2) in one syzygy \mathbf{s}_{crit} :

$$\mathbf{s}_{\text{crit}} = \sum_{\ell=k}^{n_{\max}} a_\ell \mathbf{e}_\ell - \mu \mathbf{e}_{\text{crit}} + u_i \mathbf{e}_i \tag{3}$$

where $\text{HT}(a_\ell) \mathcal{S}(r_\ell) \prec_F u_i \mathcal{S}(r_i)$ for all $\ell \in \{k, \dots, n_{\max}\}$ and $\mu \mathcal{S}(r_{\text{crit}}) \preceq_F u_i \mathcal{S}(r_i)$. As $v_G(\mathbf{s}_{\text{crit}}) = 0$ every head term of each evaluated element from \mathbf{s}_{crit} needs to be reduced. Thus we find two elements $a_\ell \mathbf{e}_\ell$ and $a_{\ell'} \mathbf{e}_{\ell'}$ in \mathbf{s}_{crit} such that

$$\text{HT}(a_\ell v_G(\mathbf{e}_\ell)) = \text{HT}(a_{\ell'} v_G(\mathbf{e}_{\ell'})).$$

This corresponds to a multiple of $\text{Spol}(r_\ell, r_{\ell'})$ where both, $u_\ell r_\ell$ and $u_{\ell'} r_{\ell'}$ have a signature lower or equal to the one of $u_i r_i$ w.r.t. \prec_F . These S-Polynomials are either rewritable/not normalized and can be rewritten in the same way without increasing their signatures or head terms, or they reduce to an element $r_{\text{red}} \in G$ such that $\mathcal{S}(r_{\text{red}}) = \mathcal{S}(\text{Spol}(r_\ell, r_{\ell'}))$ and $\text{HT}(p_{\text{red}}) < u_\ell \text{HT}(p_\ell)$, or they reduce to zero w.r.t. G . This building, reducing and deleting of new S-Polynomials stops after a finite number of steps because of the finiteness of the polynomials and their signatures.

We stop this process when we have found an element $u_{\ell_0} \mathbf{e}_{\ell_0}$ in \mathbf{s}_{crit} such that

$$u_{\ell_0} \text{HT}(v_G(\mathbf{e}_{\ell_0})) = u_i \text{HT}(p_i).$$

Thus we have found a multiple of $\text{Spol}(r_i, r_{\ell_0})$. We have to distinguish the following cases:

(a) If $u_{\ell_0}r_{\ell_0} \neq u_jr_j$ then we can represent \mathbf{s}_{crit} from Equation (3) by

$$\mathbf{s}_{\text{crit}} = \sum_{\ell=k}^{n'} b_{\ell} \mathbf{e}_{\ell} - u_{\ell_0} \mathbf{e}_{\ell_0} + u_i \mathbf{e}_i$$

where $\text{HT}(b_{\ell}p_{\ell}) < u_i \text{HT}(p_i)$ for all $\ell \in \{k, \dots, n'\}$ and $n' = n_{\max} + 1$. Note that we can assume $\mu \mathbf{e}_{\text{crit}}$ to be part of the sum. Using the evaluation we get

$$\begin{aligned} 0 &= \sum_{\ell=k}^{n'} b_{\ell} p_{\ell} - u_{\ell_0} p_{\ell_0} + u_i p_i \\ 0 &= \sum_{\ell=k}^{n'} b_{\ell} p_{\ell} + \nu_1 \text{Spol}(p_i, p_{\ell_0}) \text{ for some } \nu_1 \in \mathcal{T} \\ \Rightarrow \nu_1 \text{Spol}(p_i, p_{\ell_0}) &= - \sum_{\ell=k}^{n'} b_{\ell} p_{\ell}. \end{aligned}$$

From this equation we receive an admissible labeled t_1 -representation for $t_1 = \nu_1 \text{LCM}(\text{HT}(p_i), \text{HT}(p_{\ell_0}))$.

On the other hand we notice that $u_j \text{HT}(p_j) = u_{\ell_0} \text{HT}(p_{\ell_0})$ and thus there exists a multiple $\nu_2 \text{Spol}(r_{\ell_0}, r_j)$. This S-Polynomial is already reduced (possibly to zero) w.r.t. G or detected by the two criteria and can be rewritten in the same way, where this process has to stop after a finite number of times. In any case it will be investigated in the F_5 algorithm and we can assume it to reduce to zero or to have an admissible labeled t_2 -representation for $t_2 = \nu_2 \text{LCM}(\text{HT}(p_{\ell_0}), \text{HT}(p_j))$. Altogether we have a relation between three S-Polynomials:

$$\text{Spol}(p_i, p_j) = \nu_1 \text{Spol}(p_i, p_{\ell_0}) + \nu_2 \text{Spol}(p_{\ell_0}, p_j).$$

Possibly there are further reductions of these S-Polynomials or detections by the two criteria, but all of these do not increase the signature and do lower the head term of the polynomials.

Assuming the reduction of $\text{Spol}(r_i, r_{\ell_0})$ and $\text{Spol}(r_{\ell_0}, r_j)$ and noting the signatures of all elements which are $\preceq_F u_i \mathcal{S}(r_i)$ we have an admissible labeled t -representation of $\text{Spol}(r_i, r_j)$.

(b) If $u_{\ell_0}r_{\ell_0} = u_jr_j$ then the representation of \mathbf{s}_{crit} is given by

$$\mathbf{s}_{\text{crit}} = \sum_{\ell=k}^{n'} b_{\ell} \mathbf{e}_{\ell} - u_j \mathbf{e}_j + u_i \mathbf{e}_i$$

where $\text{HT}(b_{\ell}p_{\ell}) < u_i \text{HT}(p_i)$ for all $\ell \in \{k, \dots, n'\}$ and $n' = n_{\max} + 1$. Again using the evaluation we get

$$\begin{aligned} 0 &= \sum_{\ell=k}^{n'} b_{\ell} p_{\ell} - u_j p_j + u_i p_i \\ 0 &= \sum_{\ell=k}^{n'} b_{\ell} p_{\ell} + \text{Spol}(p_i, p_j) \\ \Rightarrow \text{Spol}(p_i, p_j) &= - \sum_{\ell=k}^{n'} b_{\ell} p_{\ell} \end{aligned}$$

Again assuming further reductions or detections by the two criteria inside $\sum_{\ell=k}^{n'} b_\ell p_\ell$ from this equality we directly receive an admissible labeled t -representation of $\text{Spol}(r_i, r_j)$ for $t = \text{LCM}(\text{HT}(p_i), \text{HT}(p_j))$.

Thus $\text{poly}(G)$ is a Gröbner basis for I . \square

Remark 3.4.

- (a) In the case of $u_i r_i$ being rewritable by λr_{rew} it is possible that $u_{\ell_0} r_{\ell_0} = \lambda r_{\text{rew}}$ also. Then by the same construction as stated in the proof we get

$$\text{Spol}(p_i, p_{\text{rew}}) = - \sum_{\ell=k}^{n'} b_\ell p_\ell.$$

In this case $\text{HT}(b_\ell) \mathcal{S}(r_\ell) \prec_F u_i \mathcal{S}(r_i) = \lambda \mathcal{S}(r_{\text{rew}})$ for all $\ell \in \{k, \dots, n'\}$. Thus $\text{Spol}(r_i, r_{\text{rew}})$ can be rewritten by a linear combination of elements in G with lower signatures, thus we have found an admissible labeled t -representation of $\text{Spol}(r_i, r_{\text{rew}})$ for $t = \text{LCM}(\text{HT}(p_i), \text{HT}(p_{\text{rew}}))$.

Note that this also includes the case where $u_{\ell_0} r_{\ell_0} = u_j r_j = \lambda r_{\text{rew}}$.

- (b) In the case $u_{\ell_0} r_{\ell_0} \neq u_j r_j$ we denote the second computed S-Polynomial

$$\text{Spol}(r_{\ell_0}, r_j) = u_{j, \ell_0} r_{\ell_0} - u_{\ell_0, j} r_j.$$

Of course it can happen that $u_{j, \ell_0} \mathcal{S}(r_{\ell_0}) \prec_F u_{\ell_0, j} \mathcal{S}(r_j)$. In this case we would compute $\text{Spol}(r_j, r_{\ell_0})$, but this would just lead to a difference in sign and would not change the arguments of the proof, hence we have omitted the distinction between these two possibilities above.

- (c) Setting $n' = n_{\text{max}} + 1$ is only necessary in the case where $n_{\text{rew}} = \max\{n_i, n_{\text{rew}}\}$ and $u_{\ell_0} r_{\ell_0} \neq \lambda r_{\text{rew}}$, i.e. if λp_{rew} is inside $\sum_{\ell=k}^{n'} b_\ell p_\ell$. Since n_{max} denotes the number of elements before r_{rew} enters G in this case, $n' = \text{rew}$. In all other cases $b_{n'} = 0$.
- (d) When building S-Polynomials inside \mathbf{s}_{crit} until we end up with $u_{\ell_0} \mathbf{e}_{\ell_0}$ the signatures do not increase. This is due to the F_5 algorithm: If there is a reductor r_{red} of an element r_{sp} , where r_{sp} denotes the possibly already reduced S-Polynomial investigated by F_5 in this step, such that there exists $u_{\text{red}} \in \mathcal{T}$ where $u_{\text{red}} \text{HT}(p_{\text{red}}) = \text{HT}(p_{\text{sp}})$ and $u_{\text{red}} \mathcal{S}(r_{\text{red}}) \succ_F \mathcal{S}(r_{\text{sp}})$ than two elements will be returned by the procedure **TopReduction**: The (in this step of the algorithm) not top-reduced element r_{sp} for which the reductor was found and a new S-Polynomial $\text{Spol}(r_{\text{red}}, r_{\text{sp}})$ with $\mathcal{S}(\text{Spol}(r_{\text{red}}, r_{\text{sp}})) = u_{\text{red}} \mathcal{S}(r_{\text{red}})$. From this point on both elements are investigated separately from each other for further reductions. So if we have defined an S-Polynomial in the beginning there is no change of its signature in the whole reduction process, and thus there is no increasing of the signatures in the proof.
- (e) Note that if we assume $u_j r_j$ to be not normalized/rewritable in the beginning instead of $u_i r_i$ the proof would work exactly the same way, it would be even easier since

$$u_\ell \mathcal{S}(r_\ell) \preceq_F u_j \mathcal{S}(r_j) \prec_F u_i \mathcal{S}(r_i) \text{ for all } \ell \in \{k, \dots, n_{\text{max}}\},$$

and due to this relation of the signatures it cannot happen that $u_{\ell_0} r_{\ell_0} = u_i r_i$.

4. EXAMPLES OF THE CRITERIA USED IN THE F_5 ALGORITHM

In this section we give some examples of the F_5 Criterion and the Rewritten Criterion. For this purpose we use the example given in both [MTM92] Section 7 and [Fau02] Section 8. We will not state the whole computations and refer to the afore-mentioned papers for more details.

Note that we do not explain in detail the difference between the computations done in both papers, but we show the critical pair the Rewritten Criterion detects to be useless whereas the criterion of Möller, Traverso and Mora stated in [MTM92] does not detect it.

The proof of Theorem 3.3 gives us a constructive explanation of the criteria which we use in every of the following computations.

In this example we want to compute the Gröbner basis of the ideal I given by

$$\begin{aligned} f_1 &= yz^3 - x^2t^2 \\ f_2 &= xz^2 - y^2t \\ f_3 &= x^2y - z^2t \end{aligned}$$

in $\mathbb{Q}[x, y, z, t]$ with degree reverse lexicographical ordering $x > y > z > t$. As agreed in Convention 2.7 $r_i := (\mathbf{e}_i, f_i)$ for $i \in \{1, 2, 3\}$.

4.1. Some Examples Of The Rewritten Criterion. We give three examples of the Rewritten Criterion. In the first example we rewrite a multiple of an element from $\{f_1, \dots, f_m\}$, in the second one we generalize this attempt for arbitrary elements in G during the computation of F_5 . In the last example we see that the Rewritten Criterion also covers direct paraphrases in which we get an admissible labeled t -representation of the investigated S-Polynomial immediately.

- (a) $P_8 = x^2r_1 - z^3r_3$ is rewritable since $x^2\mathcal{S}(r_1) = x\mathcal{S}(r_6)$. Thus for the computation of r_6 we have received a syzygy $\mathbf{s}_6 = x\mathbf{e}_1 - yz\mathbf{e}_2 - \mathbf{e}_6$ such that $x\text{MHT}_F(\mathbf{s}_6) = x^2\mathbf{e}_1$. For r_1 we get a trivial syzygy $\mathbf{s}_1 = \mathbf{e}_1 - \mathbf{e}_1$. Computing the difference of multiples of these syzygies we get

$$x^2\mathbf{s}_1 + x\mathbf{s}_6 = x^2\mathbf{e}_1 - xyz\mathbf{e}_2 - x\mathbf{e}_6$$

where $x^2\text{HT}(p_1) = xyz\text{HT}(p_2)$. So when evaluating we get a reduction of a multiple of $\text{Spol}(p_1, p_2)$:

$$x\text{Spol}(p_1, p_2) = x^2p_1 - xyzp_2 = xp_6$$

where $x\mathcal{S}(r_6) =_F x^2\mathcal{S}(r_1)$. On the other hand we compute a second multiple of an S-Polynomial with $xyzp_2$ and z^3p_3 $z\text{Spol}(p_2, p_3)$ which is already reduced to the element zp_4 . Using the relation

$$\text{Spol}(p_1, p_3) = x\text{Spol}(p_1, p_2) + z\text{Spol}(p_2, p_3)$$

$\text{Spol}(r_1, r_2)$ has an admissible labeled t -representation.

- (b) $P_{15} = xzr_6 - y^3tr_2$ is rewritable since $xz\mathcal{S}(r_6) = z\mathcal{S}(r_7)$. Again we have

$$\begin{aligned} \mathbf{s}_7 &= x\mathbf{e}_6 - z\mathbf{e}_4 - \mathbf{e}_7, \\ \mathbf{s}_6 &= \mathbf{e}_6 - \mathbf{e}_6. \end{aligned}$$

To get the related S-Polynomials we compute

$$\begin{aligned} xz\mathbf{s}_6 + z\mathbf{s}_7 &= xz\mathbf{e}_6 - xz\mathbf{e}_6 + xz\mathbf{e}_6 - z^2\mathbf{e}_4 - z\mathbf{e}_7 \\ &= xz\mathbf{e}_6 - z^2\mathbf{e}_4 - z\mathbf{e}_7 \end{aligned}$$

The next reduction would be done with $xz\mathbf{e}_6$ resp. xzp_6 . Thus we receive that $\text{HT}(x^2p_4) = \text{HT}(xzp_6)$ which leads to $z\text{Spol}(p_6, p_4)$. Clearly we also get an S-Polynomial for y^3tp_2 , namely $\text{Spol}(p_4, p_2)$ and together we receive

$$\text{Spol}(p_6, p_2) = z\text{Spol}(p_6, p_4) + \text{Spol}(p_4, p_2),$$

an admissible labeled t -representation of $\text{Spol}(r_6, r_2)$.

- (c) $P_{18} = xr_8 - y^2tr_4$ is rewritable since $x\mathcal{S}(r_8) = z\mathcal{S}(r_9)$. Note that we do not use the completely reduced polynomial r_9 which Faugère computes in the given example in [Fau02] but the reduction given from the F_5 algorithm, i.e. $r_9 = (x^3\mathbf{e}_1, -x^5t^2 + y^2z^3t^2)$. We have

$$\begin{aligned} \mathbf{s}_8 &= z\mathbf{e}_7 - \mathbf{e}_5 - \mathbf{e}_8 \\ \mathbf{s}_9 &= x\mathbf{e}_7 - z^3t\mathbf{e}_2 - \mathbf{e}_9 \end{aligned}$$

In the same way we compute

$$x\mathbf{s}_8 - z\mathbf{s}_9 = z^4t\mathbf{e}_2 - x\mathbf{e}_5 - x\mathbf{e}_8 + z\mathbf{e}_9.$$

The evaluation of the first two elements on the right-hand side of the equation is equal to $-\text{Spol}(p_5, p_2)$ which can be rewritten as y^2tp_4 such that we get that

$$\begin{aligned} v_G(x\mathbf{s}_8) - v_G(z\mathbf{s}_9) &= v_G(y^2t\mathbf{e}_4) - v_G(x\mathbf{e}_8) + v_G(z\mathbf{e}_9) = 0 \\ &\quad -\text{Spol}(p_8, p_4) + zp_9 = 0 \end{aligned}$$

such that $\text{Spol}(r_8, r_4)$ is useless for further computations.

Remark 4.1. Note that the last example above is the one reduction to zero which is not detected in [MTM92]. Using a criterion for detecting syzygies, i.e. relations between S-Polynomials, too, Möller, Traverso and Mora are using other descriptions of the polynomials and do not give the polynomials a label or signature. The syzygies and polynomials computed during the algorithm are strictly separated in their attempt, whereas in Faugère's idea the syzygies do not need to be computed, as their module head terms can be deduced by the signatures of the computed polynomials.

4.2. Some Examples Of The F_5 Criterion. In the following three examples of the F_5 Criterion are shown. The first example explains the direct paraphrase in which we can find an admissible t -representation of the investigated S-Polynomial immediately. In the second example we end with a relation between the S-Polynomial in question and two other S-Polynomials, one of them is already detected to be not normalized (first example), the other investigated as the third example.

- (a) $P_{11} = z^2r_6 - y^2tr_1$ is not normalized since $z^2\mathcal{S}(r_6) = xz^2\mathbf{e}_1$ and $xz^2 = \text{HT}(r_2)$. So we compute the syzygies

$$\begin{aligned} \mathbf{s}_{1,2} &= r_2\mathbf{e}_1 - r_1\mathbf{e}_2 \\ &= xz^2\mathbf{e}_1 - y^2t\mathbf{e}_1 - yz^3\mathbf{e}_2 + x^2t^2\mathbf{e}_2 \\ z^2\mathbf{s}_6 &= xz^2\mathbf{e}_1 - yz^3\mathbf{e}_2 - z^2\mathbf{e}_6. \end{aligned}$$

In the same way as in Section 4.1 we compute their difference to see the relations of S-Polynomials:

$$\begin{aligned} z^2\mathbf{s}_6 - \mathbf{s}_{1,2} &= y^2t\mathbf{e}_1 - x^2t^2\mathbf{e}_2 - z^2\mathbf{e}_6, \text{ where} \\ y^2t\text{HT}(p_1) &= y^3z^3t = z^2\text{HT}(p_6), \text{ and} \\ x^2t^2\text{HT}(p_2) &< y^3z^3t. \end{aligned}$$

Thus we receive the following relation of polynomials when evaluating the difference of syzygies above:

$$\begin{aligned} v_G(z^2\mathbf{s}_6) - v_G(\mathbf{s}_{1,2}) &= v_G(y^2t\mathbf{e}_1) - v_G(x^2t^2\mathbf{e}_2) - v_G(z^2\mathbf{e}_6) = 0 \\ &\quad -\text{Spol}(p_6, p_1) - x^2t^2p_2 = 0. \end{aligned}$$

It follows that $\text{Spol}(p_6, p_1)$ is reduced to zero by $x^2t^2p_2$.

- (b) Another pair which is deleted by the F_5 Criterion is the pair (r_7, r_6) which corresponds to $\text{Spol}(r_7, r_6) = (x^2y^3\mathbf{e}_1, y^3r_7 - z^4r_6)$. Since $y^3\mathcal{S}(r_7) = x^2y^3\mathbf{e}_1$ and $x^2y^3 = y^2\text{HT}(r_3)$ it is not normalized. Note that in this example also z^4r_6 is not normalized since $z^4\mathcal{S}(r_6) = xz^4\mathbf{e}_1$ and $xz^4 = z^2\mathbf{e}_2$.

Again we compute two syzygies we want to subtract from each other

$$\begin{aligned} y^2\mathbf{s}_{1,3} &= y^2r_3\mathbf{e}_1 - y^2r_1\mathbf{e}_3 \\ &= x^2y^3\mathbf{e}_1 - y^2z^2t\mathbf{e}_1 - y^3z^3\mathbf{e}_3 + y^2x^2t^2\mathbf{e}_3 \\ y^3\mathbf{s}_7 &= xy^3\mathbf{e}_6 - y^3z\mathbf{e}_4 - y^3\mathbf{e}_7 \\ &= x^2y^3\mathbf{e}_1 - xy^4z\mathbf{e}_2 - y^3z\mathbf{e}_4 - y^3\mathbf{e}_7. \end{aligned}$$

This leads to the computation of the difference of both syzygies

$$y^3\mathbf{s}_7 - y^2\mathbf{s}_{1,3} = y^2z^2t\mathbf{e}_1 - xy^4z\mathbf{e}_2 - y^3z\mathbf{e}_4 - y^3\mathbf{e}_7 - y^3z^3\mathbf{e}_3 + x^2y^2t^2\mathbf{e}_3$$

where some more S-Polynomials are computed but already at this point one can see that $y^2z^2t\text{HT}(p_1) = y^3\text{HT}(p_7)$ and we get $-y^2\text{Spol}(p_7, p_1)$. Again from the construction we also can compute that $y^2z^2t\text{HT}(p_2) = z^4\text{HT}(p_6)$ and we get $z^2\text{Spol}(p_6, p_1)$.

$\text{Spol}(r_6, r_1)$ was investigated in Case (a), $\text{Spol}(r_7, r_1)$ is also deleted by the F_5 Criterion, so we have a closer look at it in the following example. We get

$$\text{Spol}(p_7, p_6) = y^2\text{Spol}(p_7, p_1) - z^2\text{Spol}(p_6, p_1),$$

an admissible labeled t -representation of $\text{Spol}(r_7, r_6)$.

- (c) $\text{Spol}(r_7, r_1) = (x^2y\mathbf{e}_1, yr_7 - z^2tr_1)$ is not normalized since $y\mathcal{S}(r_7) = x^2y\mathbf{e}_1$ and $x^2y = \text{HT}(r_3)$. We have already computed the two syzygies

$$\begin{aligned} \mathbf{s}_{1,3} &= r_3\mathbf{e}_1 - r_1\mathbf{e}_3 = x^2y\mathbf{e}_1 - z^2t\mathbf{e}_1 - yz^3\mathbf{e}_3 + x^2t^2\mathbf{e}_3, \\ y\mathbf{s}_7 &= x^2y\mathbf{e}_1 - xy^2z\mathbf{e}_2 - yz\mathbf{e}_4 - y\mathbf{e}_7. \end{aligned}$$

So we get

$$y\mathbf{s}_7 - \mathbf{s}_{1,3} = x^2y\mathbf{e}_1 - xy^2z\mathbf{e}_2 - yz\mathbf{e}_4 - y\mathbf{e}_7 - x^2y\mathbf{e}_1 + z^2t\mathbf{e}_1 + yz^3\mathbf{e}_3 - x^2t^2\mathbf{e}_3.$$

Firstly $yz\text{Spol}(p_2, p_3)$ is built which cancels with yzp_4 such that in the end we get

$$\begin{aligned} v_G(y\mathbf{s}_7) - v_G(\mathbf{s}_{1,3}) &= -v_G(y\mathbf{e}_7) + v_G(z^2t\mathbf{e}_1) - v_G(x^2t^2\mathbf{e}_3) = 0 \\ &\quad -\text{Spol}(p_7, p_1) - x^2t^2p_3 = 0. \end{aligned}$$

Thus $\text{Spol}(r_7, r_1)$ is useless and can be deleted.

5. IMPROVING THE F_5 CRITERION?

Having a closer look at Equation (2) in the proof of Theorem 3.3 we note that instead of the not normalized case we have $\lambda\mathcal{S}(r_{\text{rew}}) =_{\text{F}} u_i\mathcal{S}(r_i)$ in the rewritable case, so we do not need to require after cancellation of the MHTs that all elements besides $u_i\mathbf{e}_i$ have signature lower than $u_i\mathcal{S}(r_i)$ w.r.t. \prec_{F} , it is enough to claim that there is no element in the syzygy having a signature bigger than $u_i\mathcal{S}(r_i)$ w.r.t. \prec_{F} . Thus the question arises if the requirement of the F_5 Criterion that $\text{index}(r_{\text{prev}}) < \text{index}(r_i)$

is too restrictive.

In the following we give a generalized definition of the F_5 Criterion due to the assumption stated above and prove that this does not give any improvement.

Definition 5.1 (Improved F_5 Criterion). Let $(r_i, r_j) \in G \times G$ be a critical pair. $\text{Spol}(r_i, r_j)$ is *not completely normalized* iff for $u_k r_k$ where $k = i$ or $k = j$ there exists $r_{\text{prev}} \in G$ such that one of the following cases holds:

- (a) $\text{Spol}(r_i, r_j)$ is not normalized.
- (b) There exists $\lambda \in \mathcal{T}$ such that

$$\begin{aligned} \text{index}(r_{\text{prev}}) &= \text{index}(r_k) =: k_0 \\ \lambda \text{HT}(p_{\text{prev}}) &= u_k \Gamma(\mathcal{S}(r_k)) \\ \text{HT}(f_{k_0}) \Gamma(\mathcal{S}(r_{\text{prev}})) &< \text{HT}(p_{\text{prev}}). \end{aligned}$$

If there exists no such $r_{\text{prev}} \in G$ then $\text{Spol}(r_i, r_j)$ is *completely normalized*.

Remark 5.2. Note that from the discussion in the beginning of this section it seems to make sense to generalize the last inequality in part (b) of Definition 5.1 to

$$\text{HT}(f_{k_0}) \Gamma(\mathcal{S}(r_{\text{prev}})) \leq \text{HT}(p_{\text{prev}}).$$

In the proof of the following lemma we show that this equality exists, but it is a trivial case which cannot be used as a criterion to detect useless critical pairs while computing Gröbner bases. See Remark 5.4 for a more detailed explanation.

Next we show that the Improved F_5 Criterion detects the same critical pairs than the F_5 Criterion. Thus Definition 5.1 is no improvement of Definition 3.1.

Lemma 5.3. *Let $(r_i, r_j) \in G \times G$ be a pair of admissible labeled polynomials, then $\text{Spol}(r_i, r_j)$ is*

$$\text{normalized} \Leftrightarrow \text{completely normalized}$$

Proof. We have to show that there exist no $\text{Spol}(r_i, r_j) \in G \times G$ and $r_{\text{prev}} \in G$ such that part (b) of Definition 5.1 is fulfilled.

Assume the contrary, for $k = i$ or $k = j$ let $\text{index}(r_{\text{prev}}) = \text{index}(r_k) = k_0$, $\lambda \in \mathcal{T}$ such that $\lambda \text{HT}(p_{\text{prev}}) = \Gamma(\mathcal{S}(r_k))$ and $\text{HT}(f_{k_0}) \Gamma(\mathcal{S}(r_{\text{prev}})) < \text{HT}(p_{\text{prev}})$. We assume that r_{prev} fulfills only part (b) of Definition 5.1. We show that there exists no such element in G . For this we have to distinguish two cases:

- (a) If $p_{\text{prev}} \in \{f_1, \dots, f_m\}$ then $p_{\text{prev}} = f_{k_0}$ as $\text{index}(r_{\text{prev}}) = k_0$. Furthermore $\Gamma(\mathcal{S}(r_{\text{prev}})) = 1$. By our assumptions

$$\begin{aligned} \text{HT}(f_{k_0}) \Gamma(\mathcal{S}(r_{\text{prev}})) &< \text{HT}(p_{\text{prev}}) \\ \Rightarrow \text{HT}(f_{k_0}) \cdot 1 &< \text{HT}(f_{k_0}) \end{aligned}$$

which is a contradiction.

- (b) If $p_{\text{prev}} \notin \{f_1, \dots, f_m\}$ then

- (i) p_{prev} is the reduction of $\text{Spol}(f_{k_0}, p_\ell)$ for some $r_\ell \in G$ such that it holds that $\text{index}(r_\ell) > k_0$. Let $u_{k_0} = \frac{\text{LCM}(\text{HT}(f_{k_0}), \text{HT}(p_\ell))}{\text{HT}(f_{k_0})}$ then it follows that $u_{k_0} = \Gamma(\mathcal{S}(r_{\text{prev}}))$ and

$$\text{HT}(f_{k_0}) \Gamma(\mathcal{S}(r_{\text{prev}})) > \text{HT}(p_{\text{prev}})$$

as the head terms of $\text{Spol}(f_{k_0}, p_\ell) = \text{HT}(f_{k_0}) \Gamma(\mathcal{S}(r_{\text{prev}}))$ cancel during the reduction step.

- (ii) p_{prev} is the reduction of $\text{Spol}(p_u, p_v)$ for $p_u, p_v \in G$. Inductively using the same argument as above we receive that

$$\text{HT}(f_{k_0})\Gamma(\mathcal{S}(r_{\text{prev}})) > \text{HT}(p_{\text{prev}}).$$

Thus both subcases contradict our assumptions about p_{prev} .

Thus we have shown that there exists no admissible labeled polynomial $r_{\text{prev}} \in G$ which fulfills part (b) of Definition 5.1. \square

Remark 5.4.

- (a) From part (a) of the proof of Lemma 5.3 we see that the only possible case which would still hold the condition on the syzygies of the proof of the main theorem, namely no signature bigger than the one of the not normalized/rewritable element, is

$$\text{HT}(f_{k_0})\Gamma(\mathcal{S}(r_{\text{prev}})) = \text{HT}(p_{\text{prev}}).$$

Note that this is only the case when $p_{\text{prev}} = f_{k_0}$ such that it leads to a trivial, not principal, syzygy, i.e.

$$\begin{aligned} \mathbf{s}_{\text{prev}, k_0} &= p_{\text{prev}} \mathbf{e}_{k_0} - f_{k_0} \mathbf{e}_{\text{prev}} \\ &= f_{k_0} \mathbf{e}_{k_0} - f_{k_0} \mathbf{e}_{k_0} \\ &= 0 \in \mathbb{K}[\underline{x}]^m. \end{aligned}$$

It follows that we do not receive a syzygy to compute relations of S-Polynomials and we cannot delete $\text{Spol}(r_i, r_j)$ from the computations of G without any other detection of further criteria.

- (b) From the point of view that the F_5 Criterion computes principal syzygies in $\mathbb{K}[\underline{x}]^m$ it is easy to see that the criterion cannot be generalized relaxing the requirement on the index of r_{prev} , as a principal syzygy with two elements of the same index will always end up in the trivial case stated above.

We have shown that the F_5 Criterion cannot be generalized in the sense of relaxing the condition on the indices.

APPENDIX A. IMPLEMENTATION IN SINGULAR

This appendix discusses another result of John Perry's and the author's joint work on the F_5 Algorithm, a freely-available library for the open-source computer algebra system SINGULAR.

A.1. Sources. This `f5_library.lib` is an implementation of a slightly improved F_5 Algorithm in SINGULAR. You can get it here:

http://www.math.usm.edu/perry/Research/f5_library.lib.

This library is implemented in the interpreted language in SINGULAR, thus it is slow, but useful for testing the algorithms behaviour. You should also download a second library, `f5ex.lib`, which consists of lots of precasted examples:

<http://www.math.usm.edu/perry/Research/f5ex.lib>.

A kernel implementation of F_5 in SINGULAR is in preparation by the author. For more information about SINGULAR visit

<http://www.singular.uni-kl.de/index.html>.

A good introduction to SINGULAR and its applications in commutative algebra resp. algebraic geometry can be found in [GP02].

A.2. Using the Implementation. The usage of `f5_library.lib` is best explained in a little example: Let us assume the computation of the example given in Section 8 in [Fau02]. Once SINGULAR is started, it awaits an input after the prompt “`⚡`”. Every statement has to be terminated by “`;`”. Firstly we have to link the two above mentioned libraries to SINGULAR, for this copy both libraries in your SINGULAR folder. As `f5ex.lib` is called internally by `f5_library.lib` it is enough to link this one. The ideal to be computed can be generated by the command `fmtm()`, which defines a basering and the ideal `i`. In the following the output of SINGULAR is accentuated by “`==>`”. The following steps should be self-explanatory, otherwise use the online manual available at

<http://www.singular.uni-kl.de/Manual/latest/index.htm>.

```
LIB 'f5_library.lib';
fmtm();
i;
==>i[1]=yz3-x2t2
==>i[2]=xz2-y2t
==>i[3]=x2y-z2t
ideal g;
g = basis(i);
==> cpu time for gb computation: 70/1000 sec
g;
==>g[1]=xz2-y2t
==>g[2]=x2y-z2t
==>g[3]=yz3-x2t2
==>g[4]=y3zt-x3t2
==>g[5]=xy3t-z4t
==>g[6]=z5t-x4t2
==>g[7]=y5t2-x4zt2
==>g[8]=x5t2-z2t5
```

Typing `help f5_library.lib`; resp. `help f5ex.lib`; one gets more information about implemented procedures and their usage.

Moreover, there is an Gröbner basis algorithm implemented using the methods and ideas for detecting useless pairs given by Gebauer and Möller in [GM88] for the purpose of comparing both algorithms. One can use it in the same way as explained above, changing `basis()` to `gm_basis()`.

REFERENCES

- [Fau02] J.C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero(F_5). *Symbolic and Algebraic Computation, Proc. Conferenz ISSAC 2002*, pages 75–83, 2002.
- [Gas08] Gash, J.M. On Efficient Computations of Grobner Bases. *Dissertation*, 2008.
- [GM88] Gebauer, R. and Möller, H.M. On an Installation of Buchberger’s Algorithm. *Journal of Symbolic Computation*, 6(2 and 3), pages 275–286, 1988.
- [GP02] Greuel, G.-M. and Pfister, G. *A SINGULAR Introduction to Commutative Algebra*. Springer Verlag, 2002.
- [MTM92] Möller, H.M., Traverso, C., and Mora, T. Gröbner bases computation using syzygies. *ISSAC 92: Papers from the International Symposium on Symbolic and Algebraic Computation*, pages 320–328, 1992.
- [Ste05] Stegers, Till. Faugère’s F_5 Algorithm Revisited. *Thesis for the degree of Diplom-Mathematiker*, 2005.

CHRISTIAN EDER, FACHBEREICH MATHEMATIK, TU KAISERSLAUTERN, POSTFACH 3049, 67653 KAISERSLAUTERN, GERMANY

E-mail address: `ederc@mathematik.uni-kl.de`